RAND

Engaging the Board

Corporate Governance and Information Assurance

Aarti Anhal, Stephanie Daman, Kevin O'Brien, Andrew Rathmell

RAND Europe

RAND

Engaging the Board

Corporate Governance and Information Assurance

Aarti Anhal, Stephanie Daman, Kevin O'Brien, Andrew Rathmell

Prepared for the Information Assurance Advisory Council (IAAC)

RAND Europe

The research described in this report was prepared for the Information Assurance Advisory Council (IAAC).

ISBN: 0-8330-3508-8

Published 2003 by the RAND Corporation
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

The INFORMATION ASSURANCE ADVISORY COUNCIL

The Information Assurance Advisory Council (IAAC) is a private sector led, cross-industry forum dedicated to promoting a safe and secure Information Society. IAAC brings together corporate leaders, public policy makers, law enforcement and the research community to address the security challenges of the Information Age.

IAAC is engaged with Government and corporate leaders at the highest levels; it produces innovative policy advice based on professional analysis and global best practice.

IAAC Corporate Sponsors

BAE SYSTEMS

symantec.

hp invent

Anite

RAND Europe

Microsoft

IAAC Government Liaison Panel

supporting UK online for business

ISC

CESG

DISCLAIMER

IAAC's recommendations do not necessarily represent the views of all of its members or sponsors, whether private sector or Government. Strategic interaction with Government is through a Government Liaison Panel.

PREFACE

This report, prepared for and funded by the Information Assurance Advisory Council, presents the results of an analysis of the relationship between corporate governance and information assurance. The objective of the study was to identify the ways in which information assurance can be embedded into corporate risk management processes in the changing UK corporate governance environment.

Corporate governance now calls for effective management of risks but board-level awareness is not yet being translated into effective controls. Based upon extensive research, consultations and testing of the findings with the corporate governance and risk management communities in the UK and abroad, this study outlines the ways in which information assurance can be embedded into corporate risk management practices and how companies can be incentivised to adopt good practices.

This report is a successor to the May 2002 IAAC Paper *Protecting the Digital Society*, which outlined three central actors in promoting information assurance – government, the private sector and citizens. This report addresses the second of these actors. This document is an overview analysis of the issues affecting the private sector, upon which IAAC is basing further analysis and actions. Three additional IAAC reports, all issued in October 2002, provide additional analysis and guidance for corporate boards:

- Benchmarking Information Assurance
- Information Assurance & Corporate Governance: What Every Director Must Know
- Insuring Digital Risk: A Roadmap for Action

The report should be of interest to boards and senior management in corporations, professionals in the legal, audit, insurance and investment sectors as well as to regulators and public policy makers concerned with promoting information assurance and modernising corporate governance.

ACKNOWLEDGMENTS

These recommendations are the result of an extensive research and consultation process undertaken by IAAC since July 2001. On behalf of IAAC, RAND Europe analysts undertook a comprehensive review of the state of the art in corporate governance and information risk management. This was supplemented with expert and stakeholder discussions at a seminar hosted by the Institute of Chartered Accountants in July 2001, an expert meeting with risk management specialists in January 2002; wider industry discussions at IAAC's January 2002 Symposium.

During the summer of 2002, IAAC issued a consultation paper to a wide audience in the UK and abroad including internal auditors, insurers, risk managers and technologists drawn from a wide cross section of the public and private sectors. This consultation was supplemented by a pilot survey focused upon IAAC members to provide in-depth information about corporate perceptions and practices. The results of this work were discussed with cross-sector representatives at IAAC's 3rd Annual Symposium in October 2002.[1]

The findings of this paper owe a great deal to the advice provided in oral and written form from dozens of participants in this research process. Particular thanks are due to the following individuals and institutions who provided detailed written comments on the paper: David Brewer; Bruno Brunskill; Daniel Dresner on behalf of National Computing Centre members; Neil Fisher; Richard Hackworth; Willie List; Angela Robinson; Andrea Shellard & Jiwan Shourie, on behalf of the Institute of Internal Auditors. Andrew Daly provided valuable comments on drafts of the paper.

Any errors of fact or interpretation are of course the responsibility of the authors.

[1] All related reports and workshop/conference materials are available at: www.iaac.org.uk

CONTENTS

EXECUTIVE SUMMARY

- The United Kingdom has an ambitious vision to build a Knowledge Society and to exploit the benefits of Information & Communication Technologies. However, this vision will only become reality if growing concerns over the lack of security in information networks are tackled. Trust and confidence are as vital to e-Commerce as they are to e-Government. Unfortunately, board-level awareness of these risks is not yet being translated into effective Information Assurance policies.

- Responsibility for management of information risk rests with company boards. Directors of UK companies are increasingly aware of the importance of Information Assurance but they are not putting in place effective controls to manage the risks.

- The market and soft regulation should be effective in ensuring that company boards manage information risks responsibly via the medium of corporate governance. Good corporate governance is critical to the successful running of a business. The Turnbull framework provides the foundation for a risk-based approach to corporate governance. However, increasing dependence upon ever more complex information systems means that more emphasis needs to be given to the information risk management element of corporate governance.

- Information Assurance is a central component of business success and of a modern corporate governance framework. Assurance of a company's information assets is critical to realisation of stakeholder value and of business potential in an economy that increasingly relies on information technology and business transactions using the Internet. However, there is still a tendency to under value the importance of IA and to ignore the benefits that can be gained from improved security and providing more information and reassurance for users.

- The involvement of senior management and the Board is a crucial factor in the success of IA strategies. Company boards need to understand the business benefits of Information Assurance; "scare stories" alone will not lead to genuine embedding of information risk management. Corporate governance guidelines, company law and sectoral regulations should be used to raise awareness amongst boards and stakeholders. Ultimately, market pressures to conform to "normal practice" are likely to be the most effective route to ensuring widespread take-up of IA policies as a way of managing information risk.

- Board level awareness requires a clear business case, backed up by simple measures of effectiveness. Positive incentives include: marketing differentiation, increased shareholder value, reduced insurance premiums and an enhanced image for Corporate Social Responsibility. Negative incentives include: damage to reputation; legal liability; reduced shareholder value.

- Once awareness is achieved, Boards need to implement effective controls. The starting point is implementation of a management standard such as ISO17799. This needs to be regarded as a minimum with which responsible organisations should comply, even if they are not certified.

- Compliance with a management standard is only a start. In order to make effective decisions about risk in today's environment, Boards need to have more sophisticated tools at their disposal - in particular ways of measuring the benefits of particular solutions so that they can gauge how much assurance they are buying. Management standards need to be complemented by audit regimes; by the generation and sharing of risk data and by increased attention to dependency risks. In addition, the insurance market needs to be stimulated by information sharing and data acquisition.

Chapter 1
Introduction

- The UK has an ambitious agenda to become a leader in the Knowledge Economy and to use ICT to transform public life
- Trust and confidence in information networks is vital to the achievement of this vision
- A clear national agenda has been articulated in *Protecting the Digital Society*
- The private sector should be capable of managing its own information risks via good corporate governance
- Corporate boards are increasingly aware of the importance of Information Assurance
- This awareness is not yet being translated into effective controls
- Boards need clear incentives and effective tools to enable them to realise the potential of the Knowledge Economy

The UK is committed to an ambitious vision in which electronic networks will create an Information Society and Knowledge Economy. Information and Communication Technologies (ICT) hold the potential to revitalise UK business, to spur economic growth and competitiveness, to revolutionise working practices and living environments as well as to transform government services and our democratic process. With the froth from the dot.com bubble out of the way, UK businesses are getting down to the serious task of harnessing ICT to make them more competitive.

However, it is clear that electronic networks will only be exploited if trust and confidence can be assured. Today, cyber-crime and information security incidents are deterring consumers and imposing costs on businesses. Tomorrow, as organisations become more dependent upon networks, insecurity will be a business critical issue.

The UK's corporate leaders are increasingly aware of the importance of managing information risk. Unfortunately, this awareness is not yet being translated into effective risk management and controls. Although almost half of UK companies suffered an information security breach in 2001, only one in 20 has achieved compliance with the international standard for information security management (ISO17799).

The gap between the business expectations being placed on electronic networks and the means by which senior management are managing the risks needs to be closed if our visions of the Information Society and Knowledge Economy are to be realised.

The Opportunity

At the national level, clear strategic visions for action have been articulated, in the form of IAAC's Manifesto: *Protecting the Digital Society* and the government's own report by Sir Edmund Burton. An important element of these visions is that Information Assurance (IA)[2] should be embedded into corporate governance practices by the boards of all organisations, in the public and private sectors alike.

[2] In this paper, the initials IA refer only to Information Assurance – Internal Audit is written in full.

In some sectors such as safety critical industries, government regulation that imposes security standards will be required. However, in most areas there is no reason why the private sector itself should not be able to effectively manage these risks. Corporate governance provides the link between the needs of society to build robust infrastructures and the needs of individual corporations to manage their risks:

> "The regulation of business and corporate risk management are inextricably linked. Regulation is one way in which risks are managed in modern societies and corporate risk management is a form of self-regulation ... Systems of "enforced self regulation" combine state and corporate regulation; they seek to penetrate the everyday life of the company and to harness its management tools in such a way as to align regulatory objectives and corporate strategy."[3]

Ongoing debates over corporate governance in the UK provide a golden opportunity to close the expectations-risk gap:

- The move to risk-based management and audit, most explicitly laid out in the Turnbull Report, provides a context for embedding management of information risk into corporate governance practices
- The Company Law Review, which aims to set out a framework for the next century, provides an opportunity to embed Information Assurance into the corporate governance framework
- Reviews of corporate governance practices in the wake of corporate disasters such as Enron, and sectoral reviews of operational risk and resiliency in the wake of September 11, have raised awareness of catastrophic risk and dependencies. These reviews provide the opportunity to broaden the focus from financial risk on the one hand and from physical risks on the other

Current Assessments of Board Awareness

Company directors and senior managers are becoming more aware of the problem of Information Assurance and security. According to the DTI's Information Security Breaches Survey 2002:

> " information security has increased in profile at board level. 73% of UK businesses now rate security as a high or very high priority to their top management or director group, as opposed to 53% back in 2000.
>
> "There is dear consensus that e-commerce systems pose more security threats than traditional systems. 61% of UK businesses believe that e-commerce systems are more of a target for fraud than non e-commerce systems, compared with only 7% that think e-commerce systems are less of a target. Most UK businesses, therefore, believe the growth of e-business activity over the last two years has resulted in increased security threats."[4]

---

[3] Bridget Hutter and Michael Power, *"Risk Management and Business Regulation"*, Financial Times Mastering Risk Series 2000

[4] DTI *" Information Security Breaches Survey 2002"*, https://www.securitysurvey.gov.uk/View2002SurveyResults.htm

However, ... this has not yet fully translated into action."[5]

This gap between Board-level awareness and effective action is borne out by other research. In the USA, a survey conducted by the National Association of Corporate Directors, the Institute of Internal Auditors and KPMG noted that only one quarter of respondents indicated that information security is on the board's agenda at least once a year[6]. In the UK, according to the Confederation of British Industry (CBI) *Cybercrime Survey 2001*, 40% of companies surveyed have yet to carry out a board-level evaluation of the risks posed by cybercrime. Yet two-thirds of companies have experienced at least one 'serious' attack. Perhaps more significantly, few of the companies in the survey, published in August 2001, planned to change their approach.

The CBI's survey concluded that, despite the Turnbull report's advocacy of top down approach, with emphasis on the wider aspects of strategy, review, personnel issues and other policies, heavy reliance continues to be placed by companies on IT security and electronic controls:

> "One might assert that many companies are failing to comply with Turnbull, but this would miss the point. The real problem is that Boards may not be giving sufficient attention to the changing business environment and how opportunities presented by the Internet can be used by companies to achieve their strategic objectives while ensuring an appropriate risk/reward ratio"[7]

In other words, even though many companies have suffered losses as a result of inadequate or poorly managed information security, there is still a tendency to see IA as a technical issue rather than one for senior management and the Board. This means that IA does not receive the support required to ensure successful company wide implementation. The risk is likely to increase as companies become ever more dependent on their information systems.

Bridging the Gap

There is a clear requirement for senior management and boards in the UK public and private sectors to treat information risk as an integral part of their responsibilities. Good management of an organisation's financial assets is accepted as a routine task; the same should go for information assets. In order to help directors and managers discharge these responsibilities, this report outlines three elements:

- Clear positive incentives
  - Boards need clear guidance on the bottom line benefits of an effective IA strategy (e.g. contribution to profitability and other corporate objectives)
- Clear negative incentives
  - Boards need clear guidance on the risks of failing to deploy an effective IA strategy (e.g. legal consequences; reputational risks)

---

[5] DTI "*Information Security Breaches Survey 2002*", https://www.securitysurvey.gov.uk/View2002SurveyResults.htm

[6] *Presenting the Information Security Case to the Board of Directors*, Audit and Control (15 November 2001)

[7] http://cbi.org.uk/ndbs/Publications.nsf/fb33050ba920aeaf8025671400362f99/c733970d9e82436680256ab9005b94c6?OpenDocument

- Tools and methods
  - Boards need the tools with which to design, implement and monitor their IA strategy (e.g. benchmarks, standards and metrics; integrated risk management technologies & processes; trained and educated people)

Chapter 2
Corporate Governance & Risk Management

- Corporate governance is the basic duty of a board of directors
- In the private and public sectors alike, corporate governance is now risk-based
- Boards have a duty to satisfy their stakeholders that all risks are being effectively managed
- Internal controls should be used to ensure that risk management is embedded throughout an organisation

Sound governance is the foundation for long-term organisational success. According to the Institute of Chartered Secretaries and Administrators, governance refers to:

> "the systems by which organisations are run and the laws, regulations and best practice with which they are required to comply". In a more general sense, governance means "ensuring compliance with regulations and the implementation of appropriate administrative procedures".[8]

Corporate Governance was defined by the 1991 Cadbury Report as: "the system by which organisations are directed and controlled. The Board of directors are responsible for the governance of their organisations".[9] More particularly, corporate governance concerns: "the relationship between the shareholders, directors and management of a company, as defined by the corporate charter, bylaws, formal policy and rule of law".[10]

Corporate Governance is the responsibility of senior management and the Board. The Board is usually made up of executive and non-executive members who have the overall duty for governance within any organisation. The responsibilities of the Board include setting the company's strategic aims, providing leadership to put them into effect, supervising the management of the business and reporting to shareholders on their stewardship. They set financial policy and oversee implementation (including the use of financial controls). The Board's actions are subject to laws, regulations and the shareholders in general meeting.

On a day-to-day basis, a senior individual within the enterprise – such as the Chief Financial Officer, the Company Secretary or the Chief Operations Officer – must stay abreast of obligations and responsibilities, provide advice on how to comply with legislation and best practice, and manage organisational systems and procedures. Internal auditors assist with a systematic and disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes[11]. The internal auditors also provide the shareholders with an objective check on the Directors' financial statements. The shareholders' role is to appoint the directors and the auditors, satisfying themselves that an appropriate governance structure is in place.

---

[8] Institute of Chartered Secretaries and Administrators (www.icsa.org.uk/about/govern.html)

[9] The UK Financial Reporting Council and The London Stock Exchange, *The Committee on the Financial Aspects of Corporate Governance – The Cadbury Report* (May 1991), Chair: Sir Adrian Cadbury.

[10] The Corporate Library (asp.thecorporatelibrary.net/glossary/default.asp?Letter=O

[11] www.theiia.org/ecm/guidance.cfm?doc_id=118

In exclusively financial terms, the Directors owe a 'duty of care'[12] to the shareholders. Although the reports of the Directors are addressed to the shareholders, they are important to a wider audience of "stakeholders", defined as shareholders, creditors, analysts, customers and consumers, employees, the supply-chain and – perhaps more widely – the Government and the public whose interests the Board may also take into account.

The trend towards demanding that companies pay attention to interests other than profit maximisation and shareholder value has gained ground in recent years under the rubric of Corporate Social Responsibility (CSR).

Corporate Governance and Risk Management

Whatever the relative priorities in a business's goals, good corporate governance involves the management of risks to an organisation with a view to ensuring the continuity of that organisation's business and its commercial success.

The 1999 *Turnbull Report* on Corporate Governance (*Internal Control: Guidance for Directors on the Combined Code*) requires companies to ensure they have a sound system of internal control and effective risk management processes which the Board regularly reviews. Companies should by now be fully compliant with the Guidance. Although primarily prepared for the listed companies of the FTSE, the Turnbull principles have been developed for the private sector in general. In a number of cases, organisations working for listed companies are expected to prove compliance with Turnbull's guidelines as part of the partner scrutiny process. Further adoption of the Turnbull principles is being encouraged via the industry regulators, e.g. the Financial Services Authority.

Good corporate governance involves three steps: identifying the risks, establishing who will be impacted by them, (in other words, to whom does a Board have a duty of care), and controlling and mitigating these risks.

As part of this process, internal controls are used to keep the company on course toward the achievement of its mission and to minimise surprises along the way. Internal control is broadly defined as a process, effected by an entity's board or directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- effectiveness and efficiency of operations
- reliability of financial reporting
- compliance with applicable laws and regulations

The Turnbull Report states the need for internal controls as follows:

> "the corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's

[12] *IS Auditing Guideline - Due Professional Care*, Booklet 14 – Information Systems Audit and Control Association (ISACA) (1999).

accountability to the company and the shareholders. To achieve this, the board should ensure the integrity of the corporation's accounting and financial reporting systems, including independent audit, and that the appropriate systems of (internal) control are in place".

Internal controls are effective if they are exercised sufficiently often to enable judgements about risk mitigation choices – these might include the transfer of some risk to third parties, the sharing of risks through joint ventures, contingency planning and the avoidance of unplanned risk-taking.

The guidance in the Turnbull Report calls on companies to ensure that their system of internal control:

- is embedded in the operations of the company
- is capable of responding to change
- includes procedures for reporting major weaknesses immediately

The guidance requires companies to:

- manage their key risks
- remedy weaknesses promptly
- review all aspects of internal control on a regular basis

A system of internal control is sound to the extent that it provides reasonable assurance that a company will not be hindered in pursuing its business objectives or in the orderly and legitimate conduct of its business, by reasonably foreseeable occurrences. This includes ensuring that fundamental financial and other controls are maintained.

The Role of the Board

Responsibility for corporate governance and risk management begins and ends with corporate leaders. As the Institute of Internal Auditors puts it:

> "The responsibility for risk management within an organisation clearly lies with the board (or equivalent) who should be responsible for setting the strategy and senior management who should be responsible for implementing the strategy, although it is also clear that everyone within an organisation bears some risk management responsibility. This responsibility and accountability is clearly set out in the Turnbull guidance and other similar pronouncements for non-listed organisations
>
> In order successfully to achieve the organisational business objectives, management should ensure that sound and effective risk management processes exist and that they are functioning as intended. Boards and audit committees have an oversight role to determine that risk management is functioning effectively within the organisation"[13]

[13] IIA-UK and Ireland – Position Statement *" The Role of Internal Audit in Risk Management"*

In the UK environment, the role of the Board is to support the governance process by exercising outside scrutiny of management. Non Executive Directors (NED) have long played a key role in this scrutiny process. Recently, however, influential voices have warned that the NED system is failing. The outgoing President of the Institute of Directors, Lord Young of Graffham, speaking at the Institute of Directors' (IoD) annual convention on 24 April 2002 questioned the assumption that part-time, non executive Directors could know enough about what is going on in their companies to spot potential difficulties. [14]

These concerns have been taken up in the wake of major corporate governance failures such as Enron and Worldcom by the Department of Trade & Industry. The Higgs review has dealt with claims that NEDs may be too close to the executives on whose Boards they sit.

Risk Management in the Public Sector

It is not just the private sector that is moving to a risk-based approach to corporate governance. In recent years, there has been a noticeable shift in the public sector towards the benefits of a risk management rather than a risk avoidance approach. Lord Sharman commented that:

> "I believe that public sector bodies should adopt Turnbull's guidelines on effective corporate governance. Essentially the Turnbull Report is all about making sure that you have got a system that identifies all the risks which face your organisation and then, having identified all those risks, that you have a sensible process in place to manage them properly.
>
> The issue of risk in the public sector is a difficult one because there isn't much of a temptation to manage risk, but rather the desire to avoid it completely. But on the other hand, clearly there is much to be gained by managing risk rather than by minimising and avoiding it" [15]

This sentiment reflects the views of influential bodies such as the International Federation of Accountants which, in October 2000, released its study *Corporate Governance in the Public Sector: A Governing Body Perspective.* The study recommended that government entities use private sector corporate governance concepts and practices to achieve their objectives more openly and effectively, and in the process, better serve their constituencies.

In a survey published by the National Audit Office (NAO) in 2001 however, although 82% of central government departments agreed that risk management was important to the achievement of their objectives, few had risk management objectives and policies[16].

Only 57% of departments had procedures for reporting risks and only a third said that regular risk reports were an effective component of managing risks in their department. However, the departments were clearly willing to change, with four-fifths saying that they supported innovative approaches to risk. The *Supporting Innovation: Managing Risk in Government Departments project* within the *Modernising Government* programme, also backs the Turnbull

---

[14] *"Non-exec role under scrutiny"* Financial Times, 25th April 2002

[15] Lord Sharman, *Sharman's Impact*, Internal Auditing & Business Risk (July 2001)

[16] http://www.IA.org.uk/knowledge/Wake1.pdf

principles. This has provided an added spur to the existing requirement to produce statements on internal financial control. By 2003/04 all central government bodies will be obliged to publish full Turnbull-style internal control statements, covering both financial and non-financial risks.

To support this process, the NAO has proposed the establishment of risk audit committees, risk management sections and working groups, the introduction of risk registers to record identified problem areas. Entities should consider mitigating controls and allocate responsibilities for risk management.

In addition to the public sector, the "third sector" has also adopted risk management. Management processes in the not-for-profit sector have been driven by the Statement of Recommended Practice (SORP 2000) issued by the Charities Commission.

Chapter 3
Information Assurance: Managing Information Age Risk

- Information assets and extended information networks are now critical to most businesses
- Turnbull requires boards to deal with safety, security and business continuity – all of which now depend on information systems
- Information Assurance is a holistic, strategic approach to ensuring the reliability, security and privacy of corporate information assets
- The e-commerce ecosystem and the consumer value chain mean that it is not enough for companies to focus only on internal controls

While Corporate Governance has long been recognised as essential to any enterprise, the 'new economy' has given rise to a greater demand for vigilance against 'new' risks. A number of factors need to be considered – these include globalisation and the increased connectivity of societies; the increased speed of production cycles; the impact of new technologies; increased demands for and awareness of regulation; a greater interdependency between businesses; and an increasing skills shortage. Added to this is the fact that company assets are changing from purely 'tangible' ones to include more 'intangible' assets – the "dematerialisation" of business.

The 1999 *Turnbull Report*, suggested that Boards should consider the following when assessing their corporate governance:

> "... areas such as customer relations, safety and environmental protection, security of tangible and intangible assets, business continuity issues, expenditure matters, accounting and financial and other reporting".[17]

The proper management of information systems, including the protection of the confidentiality, integrity and availability of information, is a central element of this 'duty of care'.

What is Information Assurance?

A communication gap has bedevilled relations between technologists and directors. Not speaking the same language, too often both groups fail to understand the needs of the other. The communication gap can only be overcome if technologists and security professionals express their concerns in business language and board members understand that "information" is not a niche activity to be left to the technologists.

Unfortunately, Boards have in the past regarded information security, or IT security, as a low level technical issue. The criticality of information to contemporary enterprises has forced a change to this perception. According to Nancy J. Wong of the US Critical Infrastructure Assurance Office (CIAO):

---

[17] *Internal Control: Guidance for Directors on the Combined Code* (Turnbull Report). Institute of Chartered Accounts in England & Wales (September 1999).

" Information security is only a part of the piece in the provision of a reliable service. It cannot, therefore, be addressed separately. Different sectors use information differently and there needs to be an implicit recognition of this in the analysis of business processes".[18]

The aim of IA is to promote trust and confidence in an organisation's information. IAAC defines Information Assurance thus:

Information Assurance is the certainty that the information within an organisation is reliable, secure and private.[19] IA encompasses both the accuracy of the information and its protection, and includes disciplines such as information security management, risk management and business continuity management.

This definition of Information Assurance is intended to focus attention on the centrality of information to holistic business assurance. The point is to alter perceptions such that Information Assurance comes to be seen not as an "add-on" but as something to be embedded throughout an organisation. The aim must be to develop a "culture of Information Assurance" in which all stakeholders, from junior employees through to the Chair understand their responsibilities.[20]

The holistic nature of IA is emphasised by the Information Systems Audit and Control Association (ISACA), which describes the sister concept of IT Governance in the following terms:

"In the information economy, successful enterprises integrate information technology (IT) and business strategies, culture and ethics in order to attain business objectives, optimise information value and capitalize on technologies. Extended enterprises, which incorporate customers, business partners, vendors, stakeholders and constituents, rely on the efficient and effective sharing of information, including goals/expectations, status and ultimately knowledge. Making this at all is mission critical to most enterprises...and making it happen as it should happen requires IT governance"[21]

Valuing Information Assurance

Information is fast becoming the most valuable corporate asset, and is essential to the very survival of a business. In order to practise IA effectively, information assets within an organisation need to be identified. So what are information assets and how should they be valued?

The DTI's *"Information Security Breaches 2002"* records that many companies believe that along with their databases, registries, and their IT systems, other information such as general data

---

[18] *Nancy J. Wong addressing the IAAC seminar 'IA & Corporate Governance'*, Institute of Chartered Accountants for England and Wales, London (19 July 2001)

[19] Information security specialists would use the terms: availability, integrity, authentication, confidentiality, and non-repudiation but these terms mean little to most directors.

[20] Although the revised OECD Guidelines on Information Security, issued in September 2002, call for a "culture of security," the intent is identical.

[21] http://www.itgovernance.org/overview.htm

about the company, Research & Development (R&D), Intellectual Property (IP), brand, reputation and complementary assets, is just as important.

> "...the survey found that people, reputation and brand, and business relationships, are rated as very important by over three-quarters of UK businesses. People have traditionally associated information security with technology and administrative processes. Effective information security is just as much about educating and managing staff, managing incidents to avoid reputational damage, and providing business partners with assurance about security"[22]

According to a recent study of this issue:

> "what determines the success of an ICT project is not so much what the company spends on buying equipment, but what it spends on complementary assets like business process design, product development, and training. These assets enable the firm to transform computers from lifeless equipment into dynamic engines of economic activity".[23]

One of the most difficult hurdles currently faced by those attempting to integrate IA considerations into corporate governance and risk management is the ability to measure the cost-benefit and Return on Investment (ROI) of IA measures. Unfortunately, Information Assurance is not always a quantifiable entity:

> "its evaluation is complicated by the fact that it can be viewed either from an electronic perspective, in which case the focus will fall solely on product and/or systems evaluation, or from a procedural and management perspective, in which case the focus will, instead, fall on the certification of the IA management process".[24]

Persistent low investment in IA amongst UK businesses is in part explained by the difficulty of calculating the value of IA investments. According to the DTI, a reasonable benchmark for expenditure on IT security is 3%-5% of an organisation's total IT budget; 73% of UK businesses spend less than 1% on information security.

> "The root cause appears to be that security is treated as an overhead rather than an investment. Business people find it difficult to apply normal commercial disciplines to IT security. Only 30% of UK businesses ever evaluate the return on investment (ROI) on their information security expenditure. ... There are genuine difficulties associated with ROI calculations for IT security. Many of the benefits are intangible or difficult to measure, such as the reduction in wasted staff time or the prevention of

---

[22] DTI "*Information Security Breaches Survey 2002*", https://www.securitysurvey.gov.uk/View2002SurveyResults.htm

[23] Pedro Solbes (Member of the European Commission Economic and Monetary Affairs), "Is there an e-Economy?", *Conference on the e-Economy in Europe: Its potential impact on EU enterprises and policies* (Brussels, 1 March 2001): europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=SPEECH/01/92|0|RAPID&lg=EN.

[24] M.M. Eloff and S.H. von Solms, "Information Security Management: An Approach to Combine Process Certification And Product Evaluation", *Computers & Security* 19 (8) (2000): 698-709.

reputational damage. It is also the case that most IT security professionals have a technical rather than commercial background, and so may lack the skills in the development of commercial business cases. "[25]

Despite the difficulty of measuring the benefits of IA, there are commercial and government bodies that recognise the criticality of IA to their businesses. One example at the top end of the security range, is the Society for World-Wide Interbank Financial Telecommunications (SWIFT), whose Director of Global Information Security stated that:

"[Information Assurance] is seen as fundamental to SWIFT's business, second only to availability."[26]

Once the criticality of a company's information assets is recognised by senior management, protecting such assets will become as routine as ensuring the doors to its buildings are locked at night. As Donn B. Parker, Consultant Emeritus at SRI International puts it:

"Security is necessary merely to enable electronic commerce to function. You do not need to know the risk of failing to decide to install it any more than you would need to know the risk of putting a lock on your front door. It's common sense, good practice, and due diligence."[27]

Information security incidents cost UK businesses billions of pounds per year:

- 44% of UK businesses have suffered at least one malicious security breach in the past year, nearly twice as many as the 2000 survey.
- The average cost of a serious security incident was £30,000. Several businesses had incidents that cost more than £500,000.
- While it may be unwise to extrapolate these figures over the whole UK population of businesses, it is reasonable to project that security incidents cost UK businesses several billion pounds during 2001.
- Yet, 56% either are not covered by insurance or do not know whether they are covered.[28]

The e-Commerce Ecosystem

There has been much discussion on the impact of the "new economy". A gathering of European business leaders convened by the European Union concluded that:

"the impact of the e-economy varies from sector to sector: it seems to be high in the most information-intensive sectors (such as digital goods, information services, information for goods, etc), where there is clear evidence of new business models and competitive behaviour. On the contrary, the impact on most so called 'traditional' industries is considered to be more gradual, due to already highly efficient industry sectors, where goods, production processes and business partners are well established

[25] DTI *"Information Security Breaches Survey 2002"*, https://www.securitysurvey.gov.uk/View2002SurveyResults.htm

[26] [1] Eric Guldentops, Director of Global Information Security of SWIFT (The Society for World Wide Interbank Financial Telecommunications), as quoted in *Computers and Security*

[27] Charles H. Le Grand, Xen Ley Parker, Thomas R Horton,"Information Security Governance" *IT Audit Forum* (15 February 2001)

[28] DTI *"Information Security Breaches Survey 2002"*, https://www.securitysurvey.gov.uk/View2002SurveyResults.htm

have long been efficient. However, value chains will undergo profound changes in traditional sectors too, notably in the business-to-business (B2B) field"[29]

According to the Organisation for Economic Co-operation & Development (OECD):

> "in terms of transactions, e-commerce is large – equivalent to the total value of industries such as pharmaceuticals and computer hardware – and growing. Current estimates put the value of e-commerce at around US$650 billion worldwide in 2000. This amount covers [B2B and B2C] transactions, though it does not include government transactions or those between consumers".[30]

While the dot.com "bust" has shown that new B2C business models can be problematic, B2B models have been much more successful as "traditional" enterprises have moved online. Interestingly, whilst many multi-national organisations have praised the merits of B2B transactions, (process efficiency, reduced production costs, accelerated information flows, and the streamlining of supply chains), UK businesses still retain some scepticism about whether e-procurement saves organisations money[31]. However, B2B e-commerce has seen the rapid growth of the electronic marketplaces. In some sectors, such as utilities, electronics, shipping and office supplies, it is expected that the majority of commerce will take place through such marketplaces.

The real impact of e-commerce is that it "creates 'new communities' where people conduct the same economic transactions that they carry out elsewhere. The difference is that a new community does not have the risk management and facilitation infrastructure that its participants are accustomed to relying on when they operate in established communities."[32]

In more technical terms, the notion of the network is changing. As Rich DeMillo noted when addressing the National Information Assurance Partnership (NIAP) Security Forum on 7 March 2001:

> "It's no longer your network; but the network of your customers, partners, your competitors and of course your adversaries. It's a network ecosystem where private and public boundaries collide, disappear, and relationship driven boundaries emerge. It's a network ecosystem that's become life critical to doing business".[33]

Once a business has acknowledged this dependency, the dangers of allowing weak components to form part of the infrastructure become clear, as this puts not only their own organisation but also their neighbours at risk. To paraphrase, the "security chain" can only be as strong as its weakest link. B2B commerce has resulted in the strengthening of processes

---

[29] European Union, *The e-economy in Europe: It's potential impact on EU enterprises and policies – Final Report*. (Brussels, 1-2 March 2001): europa.eu.int/comm/enterprise/events/e-economy/doc/e_economy_report.pdf.

[30] Vladimir López-Bassols and Graham Vickery, *E-commerce: the truth behind the web* (Directorate for Science, Technology and Industry, OECD) (14 January 2001).

[31] DTI *"Information Security Breaches Survey 2002"*, https://www.securitysurvey.gov.uk/View2002SurveyResults.htm

[32] Kathryn Vagneur discussing Corporate Governance with IAAC staff, May 2002

[33] http://www.hpnewsgram.com/newsletters/

but it has also created a desire to gain some assurance that partners in the new economy are as stable and secure as possible.

Other Stakeholders

Just as businesses need to adapt to this new economy, so do other stakeholders. Aside from being market players themselves in the Government to Business and Government to Citizen domains, governments play an important role through: encouraging competition in infrastructure markets; assuring consumers and businesses that networks are being policed and; ensuring that legal and commercial frameworks for online operations are transparent and predictable.[34]

Consumers are also learning the "new rules" surrounding e-commerce and the new economy. The 2001 *Which Online Annual Internet Survey* indicated that:

- 36% of the British public, more than 16 million people, are now surfing the Internet. This is an increase of 33% on the year before.
- Internet shopping remains a popular pastime among surfers - just under half (47%) have tried it at least once. Almost 8 million adults have made a n online purchase.

But:

- The safety of passing credit card details to online retailers remains an issue for just under half of British adults (49%). In this respect, there has been very little change in attitude from 2000 (51%).
- The Internet is still seen as a threat to one or more areas of society by the vast majority of adults, including surfers themselves. 3 in 5 adults and an even higher proportion of users (72%) feel that fraudulent activity is a key threat.
- 7 in 10 British adults do believe that the Internet should be regulated. This feeling has remained consistent over time and is felt equally by both users and non-users.[35]

Consumers' concerns reflect the fact that the new economy brings with it increased risks. Risk factors include not only the ra pid adoption of new technologies by businesses, and ever-increasing connectivity, but also globalisation, amplified demand leading to increased speed of production cycles, an ICT skills shortage, increased teleworking, more interdependency between businesses and company assets moving from the tangible to the intangible.[36]

---

[34] Vladimir López-Bassols and Graham Vickery, *E-commerce: the truth behind the web* (Directorate for Science, Technology and Industry, OECD) (14 January 2001).

[35] http://www.which.net/surveys/intro.htm

[36] European Union, *The e-economy in Europe: It's potential impact on EU enterprises and policies – Final Report.* (Brussels, 1-2 March 2001): europa.eu.int/comm/enterprise/events/e-economy/doc/e_economy_report.pdf.

Chapter 4
Elements of Corporate Information Risk Management

- ISO 17799 provides a sound means of translating the Turnbull requirements into an Information Assurance programme
- Certification is desirable but the focus should be upon achieving compliance
- Auditors and internal auditors play a vital role in managing information risk but they sometimes lack the necessary training and skills
- Risk data is lacking but there is clear business benefit in participating in information sharing initiatives that promise to fill this gap
- Dependency risk is poorly understood but is of increasing importance to business continuity
- Market pressures to conform to "normal practice" are likely to be the most effective route to ensuring widespread take-up of IA policies as a way of managing information risk

The Turnbull Report was successful in bringing the issue of internal control and risk management to the attention of the Board; its principles remain the building blocks on which good Corporate Governance is based. In addition to Turnbull's impact on listed companies, sector specific regulators such as the Financial Services Authority and Oftel are increasingly emphasising the importance of financial and operational risk management to their industries.

However, Turnbull is not prescriptive about the means companies should employ in managing their risks. This is an important principle since each sector will have its particular requirements and features. Nonetheless, the development of the new economy and of e-commerce has increased the complexity of the world in which businesses, governments and consumers operate. Additional tools and further guidance will be needed if Boards are to incorporate IA fully into their Corporate Governance framework.

The additional elements of this framework are: a Management Standard; Audit; Risk Data and; Dependency Risk.

A Management Standard

There are numerous guidelines and standards relating to Information Assurance and security. These range from the high level Guidelines on Information Security produced in 2002 in revised form by the Organisation for Economic Co-operation and Development (OECD), through risk assessment systems such as the Carnegie Mellon University (CMU)/Software Engineering Institute (SEI)'s OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), to the joint initiative by the National Security Agency (NSA) and National Institute of Standards and Technology (NIST) to promulgate minimum technical standards for system configuration.

What Boards require is a management standard that enables them to implement Turnbull in relation to information risk. The most prevalent such standard today is British Standard 7799 Code of Practice for Information Security Management, (Part I of which became International Standard 17799).

BS7799 is a comprehensive work of reference and is intended to facilitate the identification of a wide range of IA controls, which most IT environments in the industrial and commercial sectors will need. The Code contains a detailed set of controls that will satisfy the IA requirements of most IT environments across all functional domains, and a specification (BS7799 Part II), against which compliance may be assessed. It also has a certification scheme linked to it so that organisations can obtain independent confirmation that their information security management systems comply with the standard.

BS7799 therefore serves as a means of implementing the Turnbull Report's recommendations. In Government, the Cabinet Office Security Division is actively promoting this approach A report by the Public Audit Forum states that: "the Standard and its supporting guidance is a strong candidate to form the basis of inter-organisational information systems auditing"[37].

In the UK private sector, however, awareness of the standard remains poor. According to a DTI sponsored telephone survey of 1000 organisations across a wide range of UK businesses: "only 15% of people interviewed said that they were aware of the content of BS7799. In large organisations, this number only rose to 42% which is still disappointingly low."[38]

Certification, Accreditation or Compliance?

Certification can be defined as that process by which an organisation, procedure or process is tested, evaluated and rated in order to determine whether or not it complies with a certain standard. Certification has been a widespread goal in a number of quality related areas in recent years. Standards such as ISO9000 and Investors in People (IIP) have been adopted by private and public sector organisations alike.

In relation to Information Assurance, however, industry practice seems to be compliance with standards, rather than going through the formal certification process. The DTI's *Information Security Breaches Survey 2002* noted:

> "Significant numbers of UK businesses are now compliant with BS7799. 38% of those aware of the standard have already adopted it in their organisation and 18% are planning to in the near future. This means that approximately 80,000 UK businesses are now compliant with BS7799, and a further 40,000 are planning to be in the next year.
>
> What is more, 48% of those that are compliant have obtained some form of accreditation of their compliance against the standard by a third party – this equates to roughly 40,000 UK businesses. Very few of this were formally certified on the BS 7799 Certificate Register; most have simply had some form of security audit."[39]

One company that undertook full certification was the Internet Bank 'Smile.' The bank believes that its accreditation serves to reassure customers and gives the organisation the edge

---

[37] *Audit Implications of Electronic Service Delivery in the Public Sector*, Public Audit Forum http://www.public-audit-forum.gov.uk/auditimplications.pdf

[38] DTI *Information Security Breaches Survey 2002"*, https://www.securitysurvey.gov.uk/View2002SurveyResults.htm

[39] DTI *Information Security Breaches Survey 2002"*, https://www.securitysurvey.gov.uk/View2002SurveyResults.htm

on its competitors. Although such customer-based drivers are the aim of the standard, the cost and time involved in obtaining certification acts as a barrier rather than an enabler for the majority of organisations. For example, the process of obtaining accreditation for the Co-operative Bank's Internet Bank Smile involved:

> "175 pages of documentation and cost 45 consulting days, 20 of which were dedicated to risk assessment"[40].

As highlighted by Tim Voss, global IT security risk director at Reuters:

> "We comply in spirit, even if we don't have the certificate on the wall, but the benefits aren't massive in view of the cost involved in getting accreditation."[41]

After reviewing a case study of an BS7799 implementation, the IAAC Standards Working Group concluded in its Position Paper (published December 2000)[42], that the guidelines within BS7799 are based on good practice with a regular procedure for updating the standard. However the Working Group concluded that the certification process is perceived to be cumbersome and that it struggles to adapt to less mature organisations. This could be because less mature organisations do not typically have a well-defined process for information management, which is necessary for the implementation of BS7799. Smaller companies often find certification very burdensome.

Whilst companies should be encouraged to certify to the standard, it will be more practical and useful to focus upon gaining acceptance that information risk is one of the key risks that needs to be controlled in all organisations and to require Directors to provide specific confirmation through their Turnbull reporting that IA controls are in place. Directors would need to seek assurance that information risks are being managed, either by reports from management, internal auditors or by third parties. In this respect, ISO17799 could serve as a yardstick against which the organisation's IA practises could be measured. The focus should be upon compliance rather than certification.

Internal Audit

The emphasis on risk management the expansion of the role of internal auditors. The Institute of Internal Auditors has issued a Position Statement which clearly outlines the role of senior management in risk management processes, and the role that internal auditors can play in making these processes effective:

> "The role of internal audit within risk management cannot, and should not, be prescribed. The role within one organisation may change over time and the role from one organisation to another is likely to be very different.....
>
> Internal auditors' involvement in risk management should stop short of managing risks on management's behalf. However, in order to add value, it is often beneficial

---

[40] idem. It may, of course, be argued that this is not a significant investment for the return generated.

[41] Andy McCue, *Security standard is costly and time consuming*, Computing 15 November 2001

[42] For further information, please refer to the *IAAC Standards Working Group Position Paper*, December 2000, http://www.iaac.org.uk

> for internal auditors to give proactive advice or to coach management on embedding risk management processes into business activities" [43]

Just as the quality of the audit function within an organisation has become an integral part of corporate governance quality so the quality of information systems auditing is equally significant. The specialised nature of information systems auditing, and the skills necessary to perform such audits, ideally require globally applicable standards that apply specifically to information systems auditing.

ISACA produces standards, guidelines and procedures for IS auditing[44], and supports the CISA (Certified Information Systems Auditor), qualification. Both this and the CISSP, (Certified Information Systems Security Practitioner – issued by ISC2), are recognised by the IT profession and by recruiters.

In the UK, IT audit has been a feature of the Institute of Internal Auditors qualification programme since the early 1980s. IIA UK and Ireland introduced a programme of comprehensive computer audit training by offering the QiCA qualification in 1981/82. This has proved to be more attractive to internal audit students than the other two qualifications, mainly because whereas CISA and CISSP focus on IT security, QiCA has a greater focus on computer and information systems audit.

Risk Data

One of the key factors in determining risk is understanding the level of the threat. This is particularly difficult in relation to IT partly because there is so little information on which to base risk management decisions, and partly because of the ever increasing connectivity and dependency of IT systems.

> "The analysis of publicly available data found the data to be woefully inadequate for supporting computer security risk-management decisions. The best available data is only anecdotal and not representative of any specific industry or group. The need for improved data sharing, collecting, and standardizing remains as pressing today, if not more so, as it was in years past."[45]

There is therefore a pressing management need for sophisticated information sharing mechanisms and tools that will support the gathering of information security statistics to underpin risk management process. IAAC's work on the value of information sharing[46] provides a clear argument to support the benefits of information sharing initiatives, but this remains a difficult issue for most companies both in terms of being able to articulate RoI benefits of such a scheme, and result from the disclosure of security breaches and failures.

---

[43] As above

[44] More details can be found on the ISACA website, http://www.isaca.org

[45] Kevin J. Soo Hoo *"How Much Is Enough? A Risk-Management Approach to Computer Security"* June 2000 (Consortium for Research on Information Security and Policy, CRISP)

[46] IAAC *"Sharing is Protecting: A Review of IA Information Sharing Practices"* February 2002

Dependency Risk

One of the central drivers behind integrating IA into a corporate governance-oriented risk management strategy is to ensure business continuity. Boards are however becoming increasingly aware that the continuity of their business cannot be guaranteed merely by ensuring the robustness of internal controls. Organisations are increasingly dependent upon the complex web of cyber and physical infrastructures that make up contemporary society. As one observer noted of the 11 September attacks on New York,

> " The cascading fallout from the tragic events of September 11 graphically makes the business case for critical infrastructure protection. That the loss of telecommunications services can impede financial service transactions and delivery of electric power is no longer an exercise scenario. There can be no e-commerce without electricity. There can be no e-commerce without e-communications."[47]

It is now clearer than ever before that the increased connectivity and openness of computer networks increase the vulnerabilities of all organisations, to system and network failures, cyber-terrorism, and natural disasters.

IAAC's Dependencies & Risk Working Group (DRWG) conducted work on dependency risk analysis and on a three tier model involving risk assessment methodologies. In *Risk Analysis – a Review*, published in December 2000, the Working Group investigated risk assessment methods as they might apply to large-scale infrastructures across all sectors. It concluded that, although some methods and tools exist for application at the system and organisational level, none were suitable for assessing risk across dependencies.[48] Furthermore, in the DRWG study, *Critical Dependency Analysis: a global review*, published in November 2000[49], the DRWG concluded that the methods for mapping dependencies need to include political and social elements rather than just technical ones.

Conclusion

If the e-society is to function properly, IA needs to embrace large organisations and small. It is through ensuring that good IA standards and practices encompass small companies as well as large organisations that an overall governance framework will emerge that is no longer a "recommended framework", but an "obligatory" one. The standards will not have been mandated by Government, but will come about because industry and government see their value, and expect compliance with them as the "normal practise" for business. This will have the effect of ensuring that good standards and practices encompass small companies and the public sector, as well as large enterprises. Market pressure to certify to a standard is one way of achieving this. However certification does not work for all companies, and similar results can be achieved by expecting compliance.

---

[47] *Tone at the Top*, Issue 12 (November 2001) http://www.iaac.com

[48] Available from IAAC

[49] Available at the IAAC website, http://www.iaac.org.uk

Chapter 5
Incentivising the Board

- Company boards need to understand the business benefits of Information Assurance; "scare stories" alone will not lead to genuine embedding of information risk management
- Positive incentives include: marketing differentiation, increased shareholder value, reduced insurance premiums and an enhanced image for Corporate Social Responsibility
- Negative incentives include: damage to reputation; legal liability; reduced shareholder value

In many companies, senior management have not demonstrated any commitment to IA, and there is a tendency to see IA and information security as a technical issue to be delegated to the IT section by senior management. Without management support, it is very hard for an Information Security Manager to implement effective IA strategies and measures on a company-wide basis. Operating without full Board support makes it difficult to effectively deal with the different dimensions of IA, such as personnel concerns, awareness, legal considerations, policy concerns. To engage senior management, it is necessary to demonstrate clearly that IA is essential to the organisation.

IA costs money. Therefore, organisations (both public and private) need to understand the business benefit if they are to commit to such a programme. Incentives can be either positive or negative. In general, companies will do the minimum required in order to comply with negative incentives. To go beyond this, an organisation needs to see real business benefits in doing so.

Positive Incentives

Security and downside risk are often "sold" to Boards through the tried and tested approach of "Fear & Dread." A better starting point is to demonstrate the clear business benefits of effective management of information risks through a corporate wide Information Assurance strategy. There are four main incentives that can be laid out: marketing; shareholder value; lower insurance costs; and Corporate Social Responsibility.

Using IA as a Market Differentiator

One of the motivations for the Internet Bank Smile to undergo BS7799 certification, was the benefit that it could see from taking a positive approach to information security. Likewise, Rich DeMillo outlined Hewlett Packard's vision of the benefits of information security:

> "we view security as an enabler for e-strategies, a market differentiator, a secondary revenue generator, a cost savings mechanism and a key to safeguarding a company's reputation."[50]

With good planning, and the right IA measures in place, organisations can use the importance of data protection, the significance of the privacy debate and the public's concern relating to

[50] Rich DeMillo, *Security in the New Era*, http://www.hpnewsgram.com/newsletters/

the increase of cyber-crime, to increase their business, earn the trust of their customers, and give themselves a competitive edge over their competitors.

Ellen Dracos, Director of the Internet at the Home Depot in the US puts it in the following context:

> "we see information security as an extension of our customer service policy. It builds a stronger brand, it builds better loyalty, and it builds trust between our customers and us. It just makes good business sense."[51]

Positive Impact on Shareholder Values

Of itself, good corporate governance and quality management in all areas, including information assets, can impact positively on share value. According to the McKinsey Quarterly[52], two-thirds of investors said that they would pay more (up to 16%) for the stock of an organisation that was perceived to be well governed. The investors noted that well-governed companies perform better over time, thereby increasing share value. Businesses with effective governance plans manage risk better and rebound from setbacks more quickly. Investors and shareholders are only now becoming aware of the importance of managing information risks. As this awareness grows, investors are likely to reward companies that make the grade and punish those that fail.

Reductions in Insurance Premiums

The insurance industry has been addressing the issue of risk management in the e-economy but it remains immature. Loss of competitive advantage, loss of revenue, contractual violation, negative public image and loss of customer/shareholder confidence, incurred by theft of proprietary information, financial fraud, sabotage, denial of services and outside system penetration, are all risks that a company may wish to transfer or share.

Although 'risk transfer is the game',[53] for many UK businesses, this is no longer an option for their IT system related risks. Increasingly, insurance companies are tightening their general policies to exclude the rising costs of insurance payouts in the light of high profile IT related incidents.

> "As a result, most UK businesses (56%) either are not covered by any insurance policy for damage arising from IT security breaches or do not know whether they are covered. This pattern is similar for all sizes of UK businesses.
>
> To fill this gap, insurance companies are increasingly developing specific IT security policies. Although in this survey only 8% of companies currently have specific IT insurance coverage, the adoption of such policies is rapidly growing."[54]

---

51 *Information Security Governance*, Audit and Control (15 February 2001)

52 Paul Williams, *Bring the Board online with IT governance* (28 November 2001), ComputerWeekly

53 *Chris Cotterell, Safeonline, addressing the IAAC seminar 'IA & Corporate Governance'*, Institute of Chartered Accountants for England and Wales, London (19 July 2001)

54 DTI *Information Security Breaches Survey 2002"*, https://www.securitysurvey.gov.uk/View2002SurveyResults.htm

The combination of IT specific policies, and risk mitigation measures such as implementing a risk management procedure with internal controls, and regular review and reporting mechanisms to minimise or eliminate sources of business volatility, does however offer the possibility of lower insurance premiums. This can act as a powerful incentive for those senior managers looking for a concrete financial return on investment in Information Assurance.

Corporate Social Responsibility

In October 2001, the Association of British Insurers (ABI) produced a set of disclosure guidelines on social responsibility. According to Peter Montagnon, Head of Investment Affairs at the ABI, the guidelines

> "bring concerns about social responsibility into the mainstream of investment thinking and practise. We are anxious to avoid unnecessary prescription or the imposition of costly burdens. Our focus is on enhancing value in companies through effective response to risks."[55]

The ABI believes that corporate social responsibility (CSR) issues are a further set of risks - social, environmental, ethical (SEE) - that need to be managed. The ABI guidelines seek to raise the profile of such risks higher up the boardroom agenda, and, furthermore, to 'Turnbull' them so that annual reports must state how these matters are identified and dealt with by the organisation. Information Assurance will become an increasingly important element of CSR. As with environmental pollution, the security of the networks upon which society increasingly relies is a common responsibility.

IA can easily be compromised by someone else's poor practices – the chain is only as strong as its weakest link. It is therefore, in the best interests of companies to ensure that they do not become used as "jumping off" points for attacks, and that their suppliers and consumers are equally protected. Companies that are good "digital neighbours" will be rewarded.

Negative Incentives

Fear for corporate reputation, bottom line losses or even personal liability are powerful motives for action. The more far-sighted Boards will see that putting in place controls to avoid these downside risks will also led to positive benefits for the organisation. Negatives incentives include: damage to reputation; legal liability and; negative impact on shareholder value.

Damage to reputation

According to the CBI Cybercrime Survey 2001, 'loss of reputation, through adverse publicity and loss of trust, is a greater fear than financial loss for most organisations'[56]. This finding is borne out by IAAC's own survey of its members.[57] One of the key components in the successful management of reputation risk is understanding the major stakeholder expectations. In today's environment stakeholders place great value in the protection of an organisation's information.

---

[55] *A sense of responsibility*, Business Continuity (Winter 2001/2002)

[56] http://www.cbi.org.uk/ndbs/Publications.nsf/fb33050ba920aeaf8025671400362f99/c733970d9e82436680256ab9005b94c6?OpenDocument

[57] IAAC, *Benchmarking Information Assurance* (2002).

Legal Liability[58]

Responsibility for what goes wrong in cyber-space is still a developing area, but it is evolving fast. In the UK, there are clear statutory obligations upon companies and even on individual directors. The Data Protection Act, for instance, obliges organisations to apply appropriate security controls. The revised Company Law, meanwhile, will lay obligations on directors to manage Operational and Financial Risks.

Civil and contract law is also likely to play an increasing role, spurred by developments in the US. A common US view is expressed by Elliott Turrini, a US Attorney in New Jersey who maintains that civil liability, and raising the 'costs' of criminal behaviour is the way to secure computer networks.[59] Mark Grossman comments:

> "my prediction is that courts will find liability against computer owners who negligently allow their computers to be a launching pad for attacks by hackers, terrorists and others.
>
> "The company with the firewall that was breached is a sympathetic figure and as much a victim as the company attacked. The company without any security or an insufficient or 'negligent' security scheme in place is begging for a court to make it pay for its stupidity and carelessness"[60]

Negative Impact on Shareholder Value

The investment community is starting to make a concerted effort to ensure that the issue of Information Assurance raised with management because of the enormous potential for incidents that can negatively impact the valuation of a company's stock.

Examples include the hackers who attacked Amazon.com, Ebay and Yahoo in 2000. These stock prices slid between 17%-23% during the weeks that followed the attacks on their websites. To put these losses into context, in a two-week period between February 8-22, 2000, Ebay lost $4.56 billion in market capital, Amazon lost $6.67 billion, and Yahoo £17.24 billion[61]. While the broader market (S&P 500) was down about 6% over the same period, experts believe that investors punished these stocks in reaction to the company specific events surrounding the hacking incidents.

In general, markets (and stakeholders), want to have confidence that what is promised will be delivered; increasingly there is a greater emphasis on non-financial indicators of performance such as good IA and corporate governance, which can provide this assurance.

---

[58] For a detailed assessment of legal risks, see: IAAC, *What Every Director Should Know* (2002)

[59] Elliott Turrini speaking at the " *National Research Council Panel on Critical Information Infrastructure Protection and the Law*", October 22-23 2001

[60] Mark Grossman, *Liability for you if you've been hacked* (August 2000)
http://www.mgrossmanlaw.com/computerlaw.htm

[61] A. Marshall Acuff, Jnr, *Information Security Impacting Securities Valuations*, 1 August 2000
http://www.itaudit.org/forum/internet/f315in.htm

Articulating the Case

It is clear that there are benefits to be derived from properly implemented IA policies and procedures. However, IA can be expensive. Measurement tools that clearly show the Return on Investment (ROI) are immature and in need of further development. It can therefore be difficult to articulate a good business case for the expenditure required to put IA measures in place. This highlights the need for better measuring tools, and underlines the importance of using business language that is easily understood by those responsible for allocating budgets.

Chapter 6
Recommendations

- The market and soft regulation should be effective in ensuring that company boards manage information risks responsibly
- Corporate governance guidelines and company law should be used to raise awareness amongst boards and stakeholders
- Metrics and benchmarks need to be improved
- Compliance with a management standard such as ISO17799 needs to move from being best practice to being a minimum requirement
- Dependency risk needs to be better understood and managed
- The insurance market needs to be stimulated by information sharing and data acquisition
- Board level awareness requires a clear business case, backed up by simple measures of effectiveness

In order to build a safe and secure Information Society in the UK, it will be necessary for company boards to manage information risk as a routine component of their corporate governance duties. In the Knowledge Economy, good management of corporate information assets is as essential as good management of financial assets. Protection of information assets through an Information Assurance programme will yield returns both to the individual company and to society as a whole.

One means for forcing companies to adopt good Information Assurance practices would be to mandate compliance. This is beginning to happen in certain areas. The Data Protection Act forces companies and individual directors to protect personal data. The financial sector is mandated to take due account of all operational risks. The healthcare and pharmaceutical sectors are likely to be similarly affected by US regulations on this sector coming into force in 2003. In the UK, it would be possible to use the revised Company Law to mandate compliance, for example insisting on an Information Assurance report to accompany the annual financial returns.

There may come a time when such regulation is necessary but it would be far preferable to achieve the same result by a combination of soft regulation and a market-based approach. Such approaches are less likely to become "box ticking" exercises; if boards can be motivated to act of their own accord, then the substance rather than the form of information risk management will be adopted.

From the evidence outlined in Chapter 1, it does appear that efforts to raise awareness of information risk amongst boards and senior managers is working. This reflects the wider, global marketplace. As enterprise users and consumers alike have become more aware of security "bugs" in software and in the Internet as a whole, so software vendors and service providers have begun to offer more secure solutions. It will take time to build security into the information infrastructure and to embed information risk management into corporate practices, but market forces are moving in the right direction.

Nonetheless, in order to sustain this progress and to ensure that companies rapidly catch up with escalating threats and vulnerabilities, several actions will be required.

In all cases, there are actions that government can take but it will be even more important for industry users, ICT providers and professional associations to lead the way. Based on the analysis and consultation undertaken for this report, there are six priority actions:

Incorporation of IA into New Guidelines for Corporate Governance

> "Most board members are not tuned in to the arcane world of information security and its ramifications"[81]

Corporate Governance guidelines, which includes company law and sectoral regulations, currently make few direct references to Information Assurance. This is in part because information assurance was not considered to be such an important issue when the documentation was compiled - it is now time to address this omission. It is more important to use such guidelines to raise awareness and to require boards to satisfy their stakeholders that the risk is being managed.

The new Company Law should explicitly require directors to report on their management of information risks. This could be done by making this explicit in the statement of directors duties and by incorporating IA into the Operational and Financial Review for larger companies. IA audits may be a useful tool. Sectoral regulators that already lay down requirements in related areas (e.g. FSA for operational risk, Oftel/Ofcom for network security and integrity) should make explicit reference to Information Assurance. Information risks should also be included in risk reporting and auditing regimes.

Metrics

The development of metrics with which to measure IA performance for compliance, audit, insurance and investment purposes, is fundamental if IA strategies are to succeed. The development of metrics also underpins further work on standards and on other ways of encouraging consumer trust, such as codes of conduct and trustmarks.

In order to properly understand the threat, and to support the collection of the actuarial data required by the insurance industry, the benefits of information sharing need to be clearly articulated and information sharing mechanisms made more attractive. In addition, it is imperative to gain a better understanding of the threat environment, so that threats can be profiled and quantified in a manner that is useful for risk management and corporate governance. Only with these tools will Corporate Directors be able to make effective choices concerning information risk management.

To underpin the development of good corporate understanding of information risks, it is also vital to develop robust and authoritative means of measuring the value of corporate information assets and of the impact of security breaches. These metrics will often be industry specific.

---

[81] Tom Horton "*Presenting the Information Society Case to the Board*", Audit and Control (15 November 2001)

Industry sectors should work with analysts, insurers, investors and regulators to develop IA maturity models and threat and risk metrics in order to assist the creation of appropriate risk management tools. Involvement in information sharing mechanisms (such as Computer Emergency Response Teams and Information Sharing and Analysis Centres) should become an element of good practice.

Compliance with a Management Standard

Once awareness has been raised, Boards need clear guidance on the risk management methods they should adopt. ISO17799 provides a sound approach. The aim should be compliance with the standard or with a compatible, more rigorous approach. Certification should be encouraged but not mandated.

Compliance with a management standard such as ISO17799 should move from being best practice to a minimum standard. Large organisations should encourage take-up by setting standards across their value chains.

Compliance with a management standard could be encouraged by the use of trustmarks or webseals to provide assurance to customers and other stakeholders that the organisation has appropriate IA measures in place.

Globally recognised trustmarks and webseals should be developed.

Risk Management Practices: Dependency Risks

Industry and government leaders can work together to raise awareness of corporate dependencies upon extended value chains and information networks. Once boards are aware of these dependencies, they will demand tools to manage these extended risks. Integrated asset management and exception reporting will be important tools.

Further work needs to be done on the theory of, and the tools with which to measure and monitor dependency risks across value chains.

Development of Insurance Market

> "underwriters simply do not know what the risks are and therefore have no history of losses by which to set premiums"[79]

The lack of actuarial data has been a significant factor in restraining the development of a mature insurance market. However, organisations which employ risk mitigation measures and also have in place the right measures to obtain IT specific insurance, stand a greater chance of obtaining lower insurance premiums. Saving money provides a powerful incentive for senior managers to comply with the measures recommended in this paper.

---

[79] *Insights: The AON Risk Services Risk Management and Insurance Review.* Edition 1 (2000).

Support should be given to the development of appropriate actuarial techniques and collection of data, in order to encourage the development of a mature and competitive insurance market.

Board Level Awareness

To make effective decisions concerning information risk, board members first need to be made aware of the risks in appropriate business language. They then need to have more sophisticated tools at their disposal, in particular metrics by which they can gauge how much security they are buying for a level of expenditure, and what residual risk they run if some measures are left unimplemented.

Any work on metrics and tools should incorporate a requirement to provide board level material that makes clear, in business language, the risks and dependencies faced by the organisation, their impacts, and possible mitigation measures.

Appendix 1
International Perspectives

- The US has had considerable success in putting IA onto the Board agenda by focusing upon corporate governance and raising Board awareness of dependencies upon information systems
- Some other countries are following suit
- International guidelines are converging around these practices

The US Administration has promoted corporate governance as a means of improving information assurance across the board. As noted by Kenneth Juster, Under Secretary of Commerce for Export Administration:

> "The Federal government also has a supporting role to play in ensuring that a sufficient level of critical infrastructure services is available to maintain a smoothly functioning national economy. The preferred approach is to promote market rather than regulatory solutions, focusing on corporate governance and risk management, which is why management and auditor roles are so important".[62]

The importance of corporate governance was recognised in 1998 when the Critical Infrastructure Assurance Office (CIAO) chose to partner with the Institute of Internal Auditors (IIA), the National Association of Corporate Directors, the American Institute of Certified Public Accountants, and the Information Systems Audit and Control Association (ISACA). These bodies hosted a number of summits to raise awareness of the role of corporate directors in safeguarding the information assets of their organisations.

Governments are also integrating IA into their guidelines for national corporations. In South Africa, a recent study proclaimed that "[IT Security] is part of the business and it is imperative to assign responsibility for managing information security to Board level as information is a valuable and critical corporate asset."[63]

On the broader international stage, in May 1999, the Organisation for Economic Co-operation and Development (OECD) endorsed the *OECD Principles of Corporate Governance*, which constitute the chief response by governments to the G-7 Summit Leaders' recognition of corporate governance as an important pillar in the architecture of the new century's global economy. The Principles were welcomed by the G7 leaders at the Cologne summit in June 1999 and are likely to act as signposts for activity in this area by the International Monetary Fund, the World Bank, the United Nations and other international organisations.[64]

---

62 Summary of remarks by Kenneth Juster, Under Secretary of Commerce for Export Administration, at the Information Security Assurance Conference – *Plan Against Cyber Attacks* (Washington, 15 May 2001): www.itaudit.org.

63 *'Time to elevate IT Security to the Boardroom'*, eSecure South Africa (August 2000).

64 *ICGN Statement on Global Corporate Governance Principles* – Adopted July 9, 1999 at the Annual Conference in Frankfurt.